

Troubleshoot HTTP Proxies for Umbrella Roaming Client on Windows

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Overview](#)

[Symptoms](#)

[Identify if There is A Proxy](#)

[Scenario 1](#)

[Scenarios 2 and 3](#)

[Scenario 4](#)

[Add or Remove Proxy Settings](#)

[PsExec and Internet Explorer \(IE 10 or later\)](#)

[Alternative \(Registry\)](#)

[PsExec and MMC \(IE9 or earlier\)](#)

[Edit Registry](#)

Introduction

This document describes how to troubleshoot HTTP proxies for Umbrella Roaming Client on Windows.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Umbrella Roaming Client on Windows.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

On some or all computers in your Umbrella deployment, the Umbrella Roaming Client is not registering correctly. You notice this because the Umbrella Roaming Client tray icon is in a red state on a machine, or the Umbrella Roaming Client is not showing in the dashboard as expected. In addition, you are currently, or have at one point, used an HTTP proxy on your network. If a client is roaming, they have come online behind an HTTP proxy.

You currently run an HTTP Proxy: The Umbrella Roaming Client uses the "SYSTEM" user, since it runs as a system service, and you have pushed out configuration settings through Group Policy Object (GPO), or another Remote Monitoring and Management (RMM) tool, which gave user-specific HTTP proxy settings to users in your organization. In addition, you have default deny rules in your gateway firewall which do not allow HTTP/HTTPS traffic unless it is going through the proxy.

You ran an HTTP Proxy in the past: The "SYSTEM" user previously had HTTP proxy settings set at some point in the past, and now that proxy no longer exists. Because the proxy no longer exists, the SYSTEM user receives a timeout when trying to access resources over HTTP/HTTPS.

This is a helpful tool to check the SYSTEM user permissions. Complete these steps with the utility:

1. Use the utility to launch "C:\Program Files\Internet Explorer\iexplore.exe".
2. Go to <https://api.opendns.com/v2/OnPrem.Asset.>
3. Look for "1005 Missing API Key" without any security prompts. If there are prompts, ensure that UDP/TCP 443 are open to "api.opendns.com," "crl4.digicert.com," "ocsp.digicert.com" and that the DigiCert Root CA is present on the system.

If your firewall restricts unauthenticated accounts (like the SYSTEM account) from accessing the necessary sites, Umbrella registration domains need to be exempted. Since the Roaming Client calls out registration from the SYSTEM user account, this must be opened up for Umbrella's prerequisites to unauthenticated access.

Symptoms

The most common symptom is a failure to register to the Dashboard or sync with the Umbrella API. This can cause the client to either never register (and therefore not enter a protected mode), or cease updating the Dashboard.

If you see these symptoms, restart the Roaming Client service then send a diagnostic report log to support right after restarting. The client includes a proxy check which only runs at its startup.

Identify if There is A Proxy

First, check the logs.

If, in the logs, you see a log entry similar to this:

```
<#root>
```

```
2014-03-14 09:39:43 [2252] [INFO ] Trying to get Device ID from API...
```

```
2014-03-14 09:39:43 [2252] [DEBUG] Sending GET to https://api.opendns.com/v3/organizations/XXXXX/roaming
```

```
2014-03-14 09:39:43 [2252] [ERROR]
```

```
Error creating DeviceID
```

```
: The remote name could not be resolved: '
```

```
api.opendns.com'
```

This:

2014-12-08 09:25:27 [5700] [ERROR] POST failed: The operation has timed out

Or this:

2015-03-05 12:41:11 [4084] [ERROR] Error creating DeviceID: Unable to connect to the remote server

It is likely that proxy settings have something to do with this.

Scenario 1

The log shows it cannot resolve "api.opendns.com."

<#root>

The remote name could not be resolved: '

api.opendns.com'

This can be caused by several issues:

- **DNS Resolution is failing on your Network Connection:** Make sure Umbrella's DNS servers are allowed in your firewall if you block third-party DNS servers.
- **You have a proxy server that is not allowing the connection to be made:** If you have a proxy server, it is probably best to allow list "*.opendns.com" so it does not interfere with the registration or API syncing.
- **You have Port 443/TCP limited to specific IP scopes:** If you are using very strict firewall rules, you need to open 443/TCP to all outbound connections temporarily. The Umbrella Roaming Client needs to fetch the SSL certificate from GeoTrust IP/domain space.

You can read about Umbrella's specific firewall needs in Umbrella's Roaming Client Prerequisites article, which calls out HTTP proxies.

Scenarios 2 and 3

The log shows it cannot resolve "proxyserver.exampledomain.com."

<#root>

2014-03-14 09:39:43 [2252] [ERROR]

Error creating DeviceID

: The remote name could not be resolved: '

proxy1.exampledomain.com'

The log shows that it is trying to send information to the Umbrella API ("api.opendns.com"), but the resulting error says it tried to connect to "proxy1.exampledomain.com"

The reason this is happening is because the Umbrella Roaming Client uses the computer's "SYSTEM" user's proxy settings using the .NET framework call of `WebRequest.DefaultWebProxy`. This is commonly set via Group Policy Object (GPO), and unless this key is specifically deleted, can stay in the registry long term. If this proxy server no longer exists, or needs to be updated to a different host, you can modify the settings via the methods below.

Scenario 4

The log shows this message:

```
Error creating DeviceID: The underlying connection was closed: Could not establish trust relationship f
```

However, no firewall blocks are in place to UDP/TCP `cr14.digicert.com` or `ocsp.digicert.com`. If the computer is taken to a different network (say mobile hotspot), the issue continues.

Run this command to determine if there is a proxy still set here:

```
netsh winhttp show proxy
```

This proxy settings location is utilized by the Microsoft Cryptography API v2 as part of the .NET framework certificate validation. If this proxy is in place, it can cause this validation to fail. For more information, refer to the Microsoft Support article "Description of the Cryptography API proxy detection mechanism when downloading a Certificate Revocation List (CRL) from a CRL distribution point."



Note: Scenario 4 can also be caused by PCI compliance settings and .NET if TLS 1.0 is disabled. See this [Umbrella knowledge base article](#) for more information.

Add or Remove Proxy Settings



Warning: This setting is normally set using GPO or some kind of script. It is not common that this is set on an individual computer. Umbrella recommends only using this method if you want to test on an individual computer, or you believe this setting is unique to this computer. Please skip to the next method for information about using GPO for an entire group.

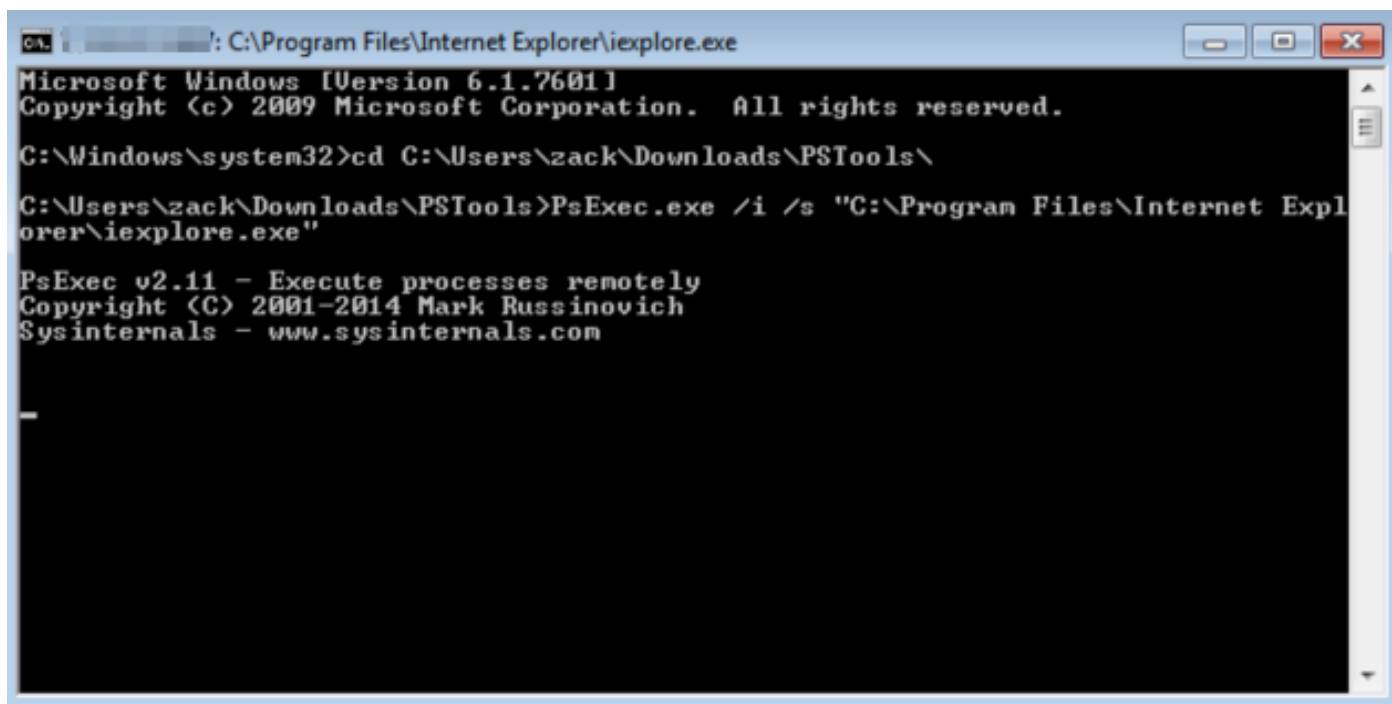
PsExec and Internet Explorer (IE 10 or later)

1. Download and extract PsExec.
2. Load an Administrative Command Prompt (**Right click > Run as Administrator**).
3. Use "cd" to change to the extracted PSTools directory.

```
cd C:\Path\To\PSTools\
```

4. Run this command to open Internet Explorer as the "SYSTEM" user:

```
PsExec.exe /i /s "C:\Program Files\Internet Explorer\iexplore.exe"
```



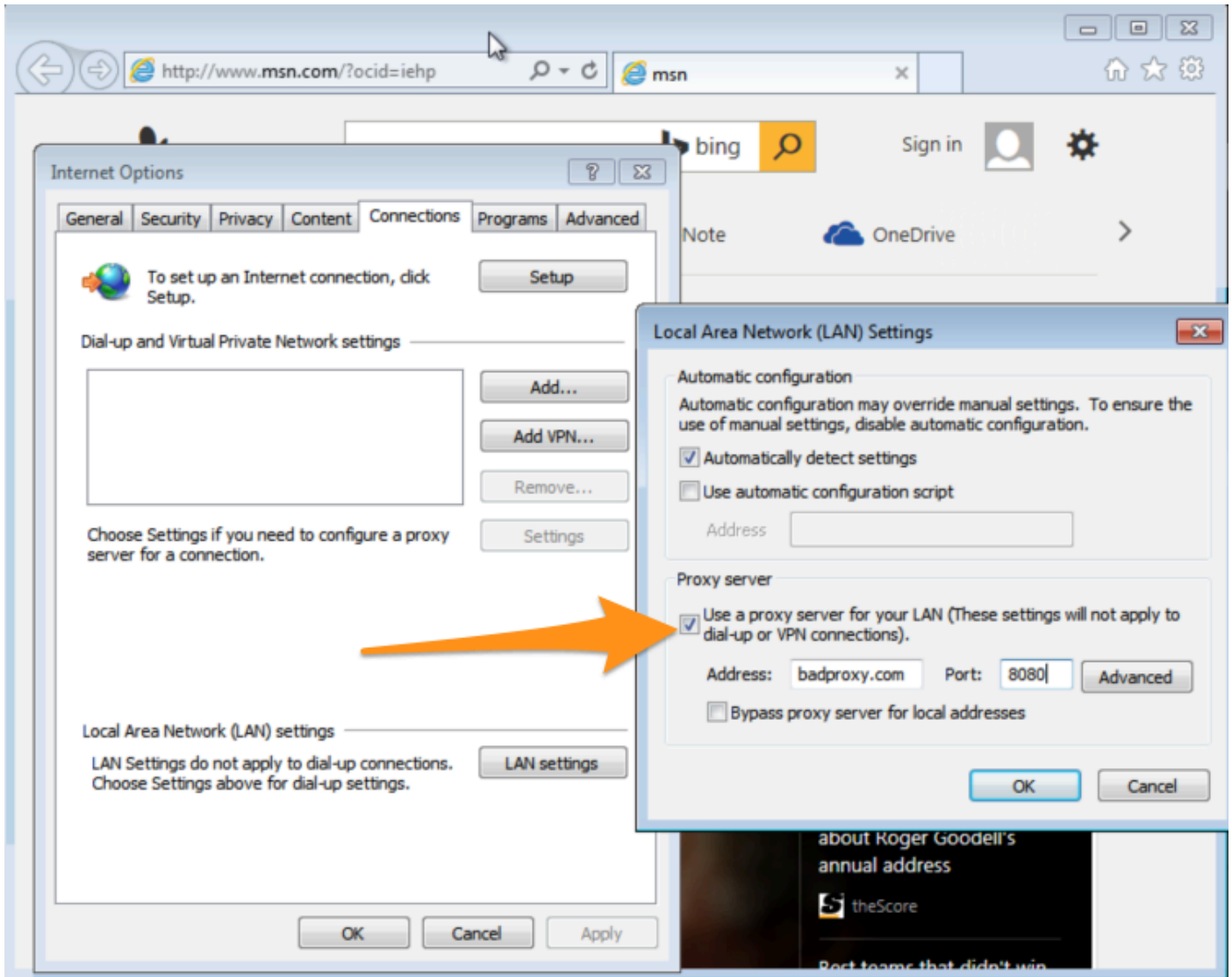
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\zack\Downloads\PSTools\
C:\Users\zack\Downloads\PSTools>PsExec.exe /i /s "C:\Program Files\Internet Explorer\iexplore.exe"

PsExec v2.11 - Execute processes remotely
Copyright (C) 2001-2014 Mark Russinovich
Sysinternals - www.sysinternals.com
```

Run PsExec.exe as the SYSTEM User

5. Open **Internet Options** from the **Settings** menu (cog) in Internet Explorer.
6. In the **Connections** tab, select **Local Area Network (LAN) Settings** and change or delete proxy settings as needed.



Change or Delete Proxy Settings in LAN Settings

7. Select **OK**, then **Apply**, and close Internet Explorer.

The Umbrella Roaming Client registers within about three minutes.

Alternative (Registry)

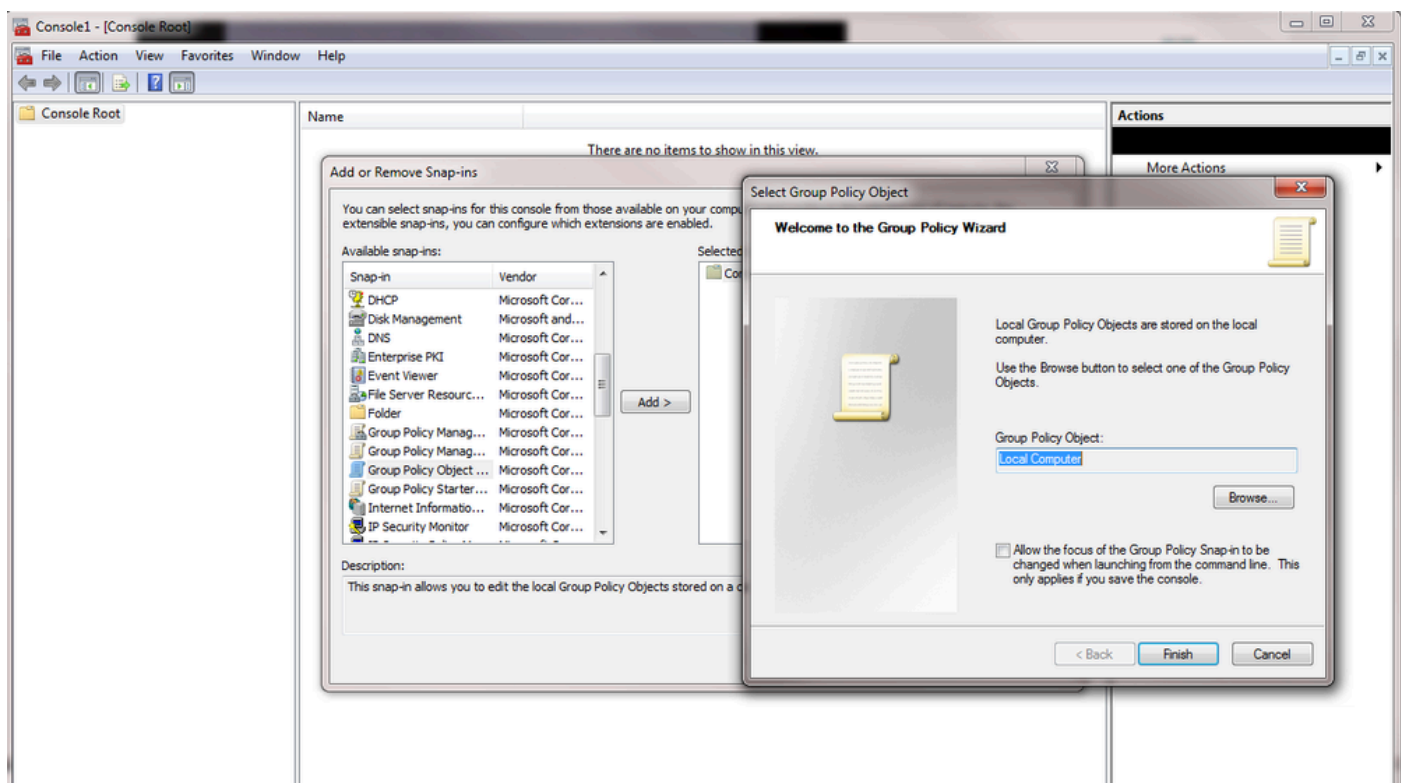
1. Check the key at **HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings** for proxy settings. If one is present, this would result in the proxy displayed earlier under the system user IE connection settings.
2. To remove in the registry, complete these steps to copy the proxy-less settings from the current user:
 1. Open up the key at **HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings** and copy the value.
 2. Copy it into the same key under **HKEY_USERS\S-1-5-18** (the SYSTEM user).
3. Restart the Roaming Client to validate if registration is successful.

PsExec and MMC (IE9 or earlier)

1. Download and extract PsExec.
2. Load an Administrative Command Prompt (**Right click > Run as Administrator**).
3. Use "cd" to change to the extracted PSTools directory.
4. Run this command:

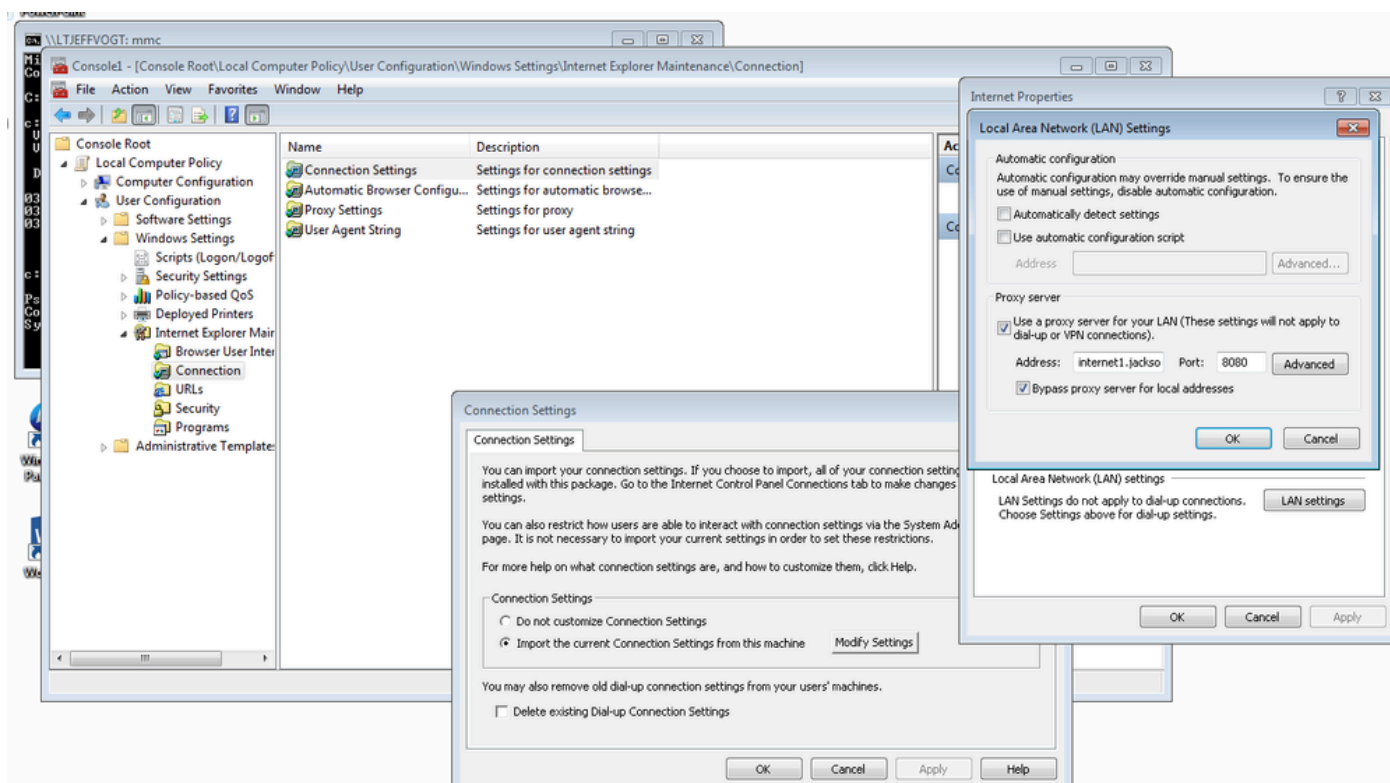
```
PsExec.exe /i /s mmc
```

5. Once the MMC loads, load the Group Policy Object snap-in.



GPO Snap-In

6. Navigate to the **Local Connection Settings** and change or delete the Proxy server information as needed.
7. Select **OK** on all menus, and the Umbrella Roaming Client then registers.



Local Connection Settings

Edit Registry

Depending on your version of Windows Server, using the earlier-mentioned steps using the MMC console and selecting the correct group works.

If your Windows Server version does not have those settings, you can modify or delete this setting via the registry in order to purge this setting at a global level (multiple computers).

HKEY_USERS

.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings

ProxyEnable (Order: 1)	show
ProxyEnable (Order: 2)	show
ProxyEnable (Order: 3)	show
DefaultConnectionSettings (Order: 4)	hide
General	hide
<div> <div>Action</div> <div>Delete</div> </div> <div> <div>Properties</div> <div> <div>Hive</div> <div>HKEY_USERS</div> </div> <div> <div>Key path</div> <div>._DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections</div> </div> <div> <div>Value name</div> <div>DefaultConnectionSettings</div> </div> </div>	
Common	show
ProxyServer (Order: 5)	hide
General	show

Delete the Connection Settings in GPO

This screenshot is an example for an older version of IE for legacy applications. Removing the proxy values from the GPO or local settings would allow the Umbrella roaming client to connect and register as the system user (subject to these IE proxy settings).

Name	Type	Data	
(Default)	REG_SZ	(value not set)	
EnableNegotiate	REG_DWORD	0x00000001 (1)	
IE5_UA_Backup_...	REG_SZ	5.0	
ProxyEnable	REG_DWORD	0x00000001 (1)	
ProxyServer	REG_SZ	pmfsrvisa:8080	
User Agent	REG_SZ	Mozilla/4.0 (compatible; MSIE 8.0; Win32)	
ZonesSecurityU...	REG_BINARY	d2 80 a9 04 3f 04 ca 01	

Remove Proxy Values

If either of these methodologies does not work, please open an Umbrella Support ticket through the dashboard and refer to this article.